

# SPLK-1003<sup>Q&As</sup>

Splunk Enterprise Certified Admin

**Pass Splunk SPLK-1003 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/splk-1003.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Where can scripts for scripted inputs reside on the host file system? (select all that apply)

- A. \$SFLUNK\_HOME/bin/scripts
- B. \$SPLUNK\_HOME/etc/apps/bin
- C. \$SPLUNK\_HOME/etc/system/bin
- D. \$S?LUNK\_HOME/etc/apps/bin\_

Correct Answer: ACD

"Where to place the scripts for scripted inputs. The script that you refer to in \$SCRIPT can reside in only one of the following places on the host file system: \$SPLUNK\_HOME/etc/system/bin \$SPLUNK\_HOME/etc/apps/bin \$SPLUNK\_HOME/bin/scripts As a best practice, put your script in the bin/ directory that is nearest to the inputs.conf file that calls your script on the host file system."

---

**QUESTION 2**

An index stores its data in buckets. Which default directories does Splunk use to store buckets? (Choose all that apply.)

- A. bucketdb
- B. frozendb
- C. colddb
- D. db

Correct Answer: CD

Reference: <https://docs.splunk.com/Documentation/Splunk/8.2.1/Indexer/Bucketsandclusters>

---

**QUESTION 3**

The CLI command splunk add forward-server indexer: will create stanza(s) in which configuration file?

- A. inputs.conf
- B. indexes.conf
- C. outputs.conf
- D. servers.conf

Correct Answer: C

The CLI command "Splunk add forward-server indexer:" is used to define the indexer and the listening port on forwards. The command creates this kind of entry "[tcpout-server://:]" in the outputs.conf file.

Reference: <https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configureforwardingwithoutoutputs.conf>  
<https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Enableareceiver>

---

## QUESTION 4

What options are available when creating custom roles? (select all that apply)

- A. Restrict search terms
- B. Whitelist search terms
- C. Limit the number of concurrent search jobs
- D. Allow or restrict indexes that can be searched.

Correct Answer: ACD

<https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits> "Set limits for concurrent scheduled searches. You must have the edit\_search\_concurrency\_all and edit\_search\_concurrency\_scheduled capabilities to configure these settings."

---

## QUESTION 5

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

- A. Deployer
- B. Cluster master
- C. Deployment server
- D. Search head cluster master

Correct Answer: A

[SPLK-1003 Practice Test](#)

[SPLK-1003 Study Guide](#)

[SPLK-1003 Braindumps](#)